E-DIMAS: Jurnal Pengabdian kepada Masyarakat, 15(4), 850-855
ISSN 2087-3565 (Print) dan ISSN 2528-5041 (Online)
Available Online at http://journal.upgris.ac.id/index.php/e-dimas

Peningkatan Digital Security Awareness pada Komunitas Read Aloud Jogja

Subektiningsih[1], Kartika Sari Yudaninggar[2]
[1,2]Universitas Amikom Yogyakarta
[1]subektiningsih@amikom.ac.id

Received: 31 Agustus 2023; Revised: 2 November 2024; Accepted: 4 Desember 2024

Abstract

Increased understanding of the importance of security activation factors and information security aspects related to various owned and published content. Apart from that, administrators from the Read Aloud Jogja Community also need to understand the security of the devices used. Increasing awareness of digital security is not only through the online media used, but also in the devices used to access it. Therefore, Community administrators need to understand the device security guidelines that need to be implemented. Increasing awareness of digital security will be carried out through workshops. After the implementation of the seminar, 100% of the participants experienced increased awareness of digital security threats with varying levels of understanding. In this case 80% of participants became more aware of the threat of crime and how to deal with it. Meanwhile, 20% of the participants became aware of the threat of digital crime, but were unable to implement ways to deal with it. 80% of participants will ensure the correctness of information from unknown numbers or sources. After the seminar was held, 100% of participants implemented Two Factor Authentication (2fa) for data protection and 100% of them agreed not to click on links originating from uncredible sources.

Keywords: *digital; security; awareness; Read Aloud; community*

Abstrak

Peningkatan pemahaman tentang pentingnya faktor aktivasi keamanan dan aspek keamanan informasi yang berkaitan dengan berbagai konten yang dimiliki maupun dipublikasikan. Selain itu, pengurus dari Komunitas Read Aloud Jogja juga perlu memahami tentang keamanan dari perangkat yang digunakan. Peningkatan kesadaran akan keamanan digital ini bukan hanya melalui media online yang digunakan, namun juga dalam perangkat yang digunakan untuk mengakses. Oleh sebab itu, pengurus Komunitas perlu memahami tentang *security guideline* perangkat yang perlu diterapkan. Peningkatan kesadaran keamanan digital ini akan dilakukan melalui workshop. Setelah pelaksanaan seminar 100% peserta mengalami peningkatan kesadaran terhadap ancaman keamanan digital dengan level pemahaman yang bervariasi. Dalam hal ini 80 % peserta menjadi lebih sadar akan ancaman kejahatan dan cara menanggulanginya. Sedangkan 20% peserta menjadi mengetahui tentang ancaman kejahatan digital, namun belum dapat menerapkan cara menanggulanginya. 80% peserta akan memastikan kebenaran informasi dari nomor atau sumber yang tidak diketahui. Setelah dilaksanakan seminar, 100% peserta menerapkan *Two Factor Authentication (2fa)* untuk perlindungan data dan 100% mereka setuju untuk tidak meng-klik link yang berasal dari sumber tidak kredibel.

Kata Kunci: digital; security; awareness; Read Aloud; komunitas

A. PENDAHULUAN

Komunitas Read Aloud Jogja adalah komunitas yang bergerak di bidang Literasi, khususnya pada anak-anak. Visi Komunitas Read Aloud Jogja yaitu membangun kebiasaan membacakan nyaring setiap hari, di lingkungan keluarga dan para pendidik yang berada di area Daerah Istimewa Yogyakarta. Komunitas Read Aloud Jogja adalah komunitas nirlaba yang bergerak di bidang literasi. Komunitas Read Aloud memiliki tujuan untuk menumbuhkan kecintaan membaca dan meningkatkan keterampilan literasi khususnya pada anak-anak di wilayah Daerah Istimewa Yogyakarta. Komunitas Read Aloud Jogja membayangkan masa depan anak Indonesia memiliki keterampilan membaca yang diperlukan untuk mencapai potensi terbaik mereka. Komunitas Read Aloud Jogja percaya kegiatan membacakan nyaring dapat mengubah kehidupan menjadi lebih baik seperti slogan yang dinarasikan, yaitu "membacakan nyaring 15 menit, setiap anak, setiap orang tua, setiap hari".

Komunitas Read Aloud Jogja menggunakan media digital dan memanfaatkan internet untuk mempublikasikan berbagai informasi dan kegiatan yang dilakukan. Pemanfaatan internet ini juga seiring dengan pengguna internet di Indonesia telah mencapai 202,35 juta orang yang berarti 76,8 persen dari penduduk indonesia telah memanfaatkan internet (Darmawan, n.d.). Hampir 94,9 persen pengguna internet di Indonesia mengakses internet melalui *smartphone* (Maulida, n.d.; Social, 2022). Indonesia juga menjadi negara kedua yang paling lama berselancar menggunakan *smartphone* yaitu dengan total penggunaan durasi internet harian sebanyak 59,4% (Maulida, n.d.; Social, 2022). Pengguna internet juga dihimbau untuk dapat berhati – hati saat klik situs atau link dari sumber yang tidak terpercaya (Flatworld Solutions, n.d.; Kominfo, 2013). Sehingga, para pengurus komunitas Read Aloud Jogja juga perlu memperhatikan halaman website atau media digital yang digunakan. Dalam hal ini, Komunitas memanfaatkan media digital Instagram untuk mengelola informasi. Dalam melakukan manajemen konten dan pengaturan Instagram dilakukan oleh pengurus. Jumlah pengurus Read Aloud Jogja berjumlah 10 orang yang juga menjadi pengelola konten instagram. Oleh sebab itu, ke semua pengurus tersebut mengetahui *username* dan *password* yang *login*.

Data untuk login tersebut perlu dijaga kerahasiaanya. Selain itu, keamanan dalam 2 tahap pengamanan perlu diterapkan. Hal ini juga disebabkan karena perangkat yang digunakan oleh pengurus berbeda-beda. Mengaktifkan *Two Factor Authentication (2fa)* menjadikan sistem akan mengirimkan kode verifikasi melalui metode yang dipilih. Keamanan menjadi hal yang perlu diperhatikan ketika akun dikelola beberapa pengurus yang berbeda.

Keamanan menjadi hal penting dikarenakan dalam media digital terdapat berbagai informasi yang perlu dijaga. Terdapat 3 aspek keamanan informasi yang perlu dipertimbangkan *Confidentiality* (C), *Integrity* (I), dan *Availability* (A) dikenal sebagai triad CIA, terkadang juga disebut sebagai triad AIC untuk menghindari kebingungan dengan istilah *Central Intelligence Agency*. Sebagian besar kebijakan keamanan informasi berfokus pada perlindungan tiga aspek utama dari data dan informasinya, setiap tujuan membahas aspek yang berbeda dalam memberikan perlindungan terhadap informasi.

Confidentiality atau Kerahasiaan mencakup spektrum kontrol akses dan tindakan yang melindungi informasi agar tidak disalahgunakan oleh akses yang tidak sah. Cara ideal untuk menjaga kerahasiaan data dan mencegah pelanggaran data adalah dengan menerapkan pengamanan. Setiap informasi yang dimiliki perusahaan memiliki nilai, terutama di dunia saat ini. Baik itu data keuangan, nomor kartu kredit, rahasia dagang, atau dokumen hukum, semuanya membutuhkan kerahasiaan yang tepat. Dengan kata lain, hanya orang yang berwenang untuk melakukannya yang dapat mengakses data sensitif. Kegagalan dalam menjaga kerahasiaan berarti seseorang yang seharusnya

tidak memiliki akses telah berhasil mendapatkan akses ke informasi pribadi. Melalui perilaku yang disengaja atau tidak disengaja, kegagalan dalam kerahasiaan dapat menyebabkan kerusakan.

Integrity mengacu pada keakuratan dan kelengkapan data. Kontrol keamanan yang berfokus pada integritas dirancang untuk mencegah data diubah atau disalahgunakan oleh pihak yang tidak berwenang. Integritas melibatkan pemeliharaan konsistensi dan kepercayaan data selama seluruh siklus hidupnya. Data tidak boleh diubah saat transit, dan langkah pencegahan harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang yang tidak berwenang.

Availability terkait dengan ketersediaan data berarti bahwa informasi dapat diakses oleh pengguna yang berwenang. Hal ini memberikan jaminan bahwa sistem dan data dapat diakses oleh pengguna yang diautentikasi kapan pun mereka dibutuhkan. Mirip dengan kerahasiaan dan integritas, ketersediaan juga memiliki nilai yang tinggi.

Kerahasiaan, integritas, dan ketersediaan komunikasi dalam media digital menghadapi ancaman yang bersifat teknis dan nonteknis dalam banyak hal yang berbeda level. Pengguna terkadang tidak mempunyai informasi yang memadai sehubungan dengan ancaman yang dapat dihadapi, sehingga tidak mengikuti praktik terbaik untuk melindungi perangkat *mobile* mereka. Selain itu, terdapat pengguna yang tidak terbiasa dengan semua fungsi, fitur yang ditawarkan oleh perangkat *mobile* yang dimiliki, sedangkan GUI tidak selalu membantu meningkatkan keamanan.

Oleh karena itu, masalahnya bukan hanya teknis, tetapi meluas ke pemahaman dan kesadaran pengguna. Untuk mengatasi ancaman, hal pertama yang dapat dilakukan adalah meningkatkan pemahaman dan kesadaran. Pengguna juga perlu memeriksa perizinan terhadap aplikasi sebelum penginstalan. Sistem perizinan akan memberi pengguna sebuah opsi untuk memeriksa permintaan izin aplikasi tersebut sebelum penginstalan. Sebagian pengguna memiliki pengetahuan tentang apa yang didukung oleh semua permintaan izin ini, namun sebagian yang lain mengabaikan. Hal ini dapat mengurangi perlindungan terhadap risiko yang mungkin diterima pengguna.

Berdasarkan uraian tersebut diperlukan peningkatan pemahaman tentang pentingnya faktor aktivasi keamanan dan aspek keamanan informasi yang berkaitan dengan berbagai konten yang dimiliki maupun dipublikasikan. Selain itu, pengurus dari Komunitas Read Aloud Jogja juga perlu memahami tentang keamanan dari perangkat yang digunakan. Peningkatan kesadaran akan keamanan digital ini bukan hanya melalui media online yang digunakan, namun juga dalam perangkat yang digunakan untuk mengakses.

Oleh sebab itu, pengurus Komunitas perlu memahami tentang *security guideline* perangkat yang perlu diterapkan. Peningkatan kesadaran keamanan digital ini akan dilakukan melalui workshop. Pengurus akan langsung mempraktikkan aturan keamanan perangkat yang perlu diterapkan dan keamanan informasi yang perlu diperhatikan. Harapannya melalui kegiatan ini terjadi peningkatan dari para pengurus akan pentingnya keamanan digital yang berkaitan dengan aspek informasi, media online, dan perangkat yang digunakan.

B. PELAKSANAAN DAN METODE

Metode pelaksanaan kegiatan digambarkan dalam bentuk tabel yang disinkronkan dengan permasalahan dan target luaran. Adapun metode pelaksanaan kegiatan disajikan pada Tabel 1.

Tabel 1. Metode Pelaksanaan Kegiatan

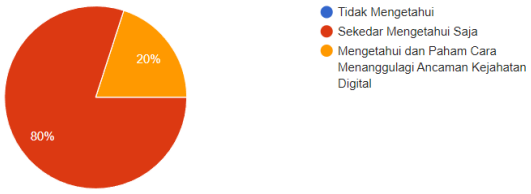
Permasalahan	Solusi dan Metode Pelaksanaan
Media digital Komunitas Read Aloud Jogja dikelola oleh 10 pengurus dengan perangkat yang berbeda dan tingkat kesadaran keamanan digital yang bervariasi.	Seminar dengan materi pembahasan tentang pentingnya keamanan digital yang berkaitan dengan *threat* (ancaman), *vulnerability* (kerentanan), dan *risk* (resiko).

Permasalahan	Solusi dan Metode Pelaksanaan
Komunitas perlu memahami tentang aspek keamanan informasi (*confidentiality*, *integrity*, *availability*) dalam mengelola dan mengakses konten	Seminar dengan materi pembahasan aspek informasi (*confidentiality*, *integrity*, *availability*)
Komunitas perlu memahami tentang *security guideline* perangkat yang perlu diterapkan untuk meningkatkan standar dasar keamanan.	Seminar dengan materi pembahasan *security guideline* dan Teknik dasar keamanan untuk diterapkan pada perangkat

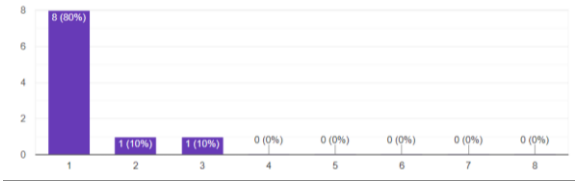
C. HASIL DAN PEMBAHASAN

Dalam pemanfaatan *smartphone* dan internet perlu memperhatikan keamanan data dan *device* yang digunakan. Oleh sebab itu, dilaksanakan seminar untuk mewujudkan kesadaran keamanan dalam pemanfaatan teknologi. Seminar ini berlangsung pada hari Kamis, 20 Juli 2023 yang dihadiri oleh 10 peserta dari Keanggotaan Komunitas dan 5 orang peserta dari Kepengurusan Komunitas Read Aloud Jogja. Seminar dilangsungkan di Grhatama Pustaka Yogyakarta, Dinas Perpustakaan dan Arsip Daerah Istimewa Yogyakarta. Acara seminar berlangsung pada pukul 13.00 – 15.30 dengan model seminar penyampaian materi dilanjutkan dengan tanya jawab dan diskusi. Dalam pelaksanaan seminar ini diawali dengan pengisian pre-test yang dapat diakses pada alamat https://s.id/sebelumacara.

Tujuan dari pelaksanaan pre-test ini adalah untuk melihat tingkat kesadaran keamanan dari peserta seminar. Dan hasilnya adalah semua peserta setuju bahwa keamanan digital sangat penting, namun baru 80 % yang sekedar mengetahui ancaman dan tindak kejahatan yang dapat terjadi di dunia maya, sedangkan 20% menyatakan sama sekali tidak mengetahuinya. Hasil ini ditunjukkan pada Gambar 1. Selain itu, 80% dari peserta cenderung sangat tertarik dengan pesan yang memberikan iming-iming hadiah atau uang walaupun nomor yang memberikan pesan tersebut tidak diketahui. Hasil ini ditunjukkan dalam Gambar 2. Dalam hal ini dapat disimpulkan bahwa tingkat kesadaran terhadap ancaman keamanan digital peserta masih rendah. Oleh sebab itu, dilakukan seminar yang berisi kasus-kasus serangan yang terjadi di dunia maya, cara menanggulanginya serta cara mendeteksi valid atau tidaknya suatu informasi.



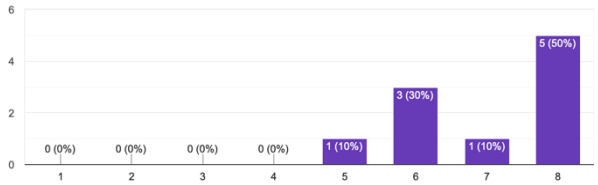
Gambar 1. Pengetahuan Ancaman Tindak Kejahatan Digital



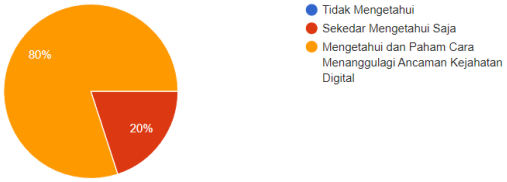
Gambar 2. Tingkat Keinginan Untuk Mendapatkan Hadiah Atas Iming-Iming Nomor Tidak Dikenal

Setelah acara seminar selesai dilanjutkan dengan post-test yang diakses melalui https://s.id/setelahacara. Terdapat peningkatan dari pengetahuan dalam keamanan digital, hal ini dibuktikan dengan 90 % yang menyatakan sangat meningkat pemahamannya (dalam skala 6,7,8 dari 8), dan 10 % cukup mengalami peningkatan pemahaman (dalam skala 5). Hasil ini ditunjukkan pada Gambar 3. Selanjutnya, Terdapat juga peningkatan kesadaran atas ancaman dan tindak kejahatan di dunia maya. Kondisi awal, 80 % peserta hanya mengetahui saja terhadap ancaman di dunia maya, maka setelah seminar menjadi lebih mengetahui jenis ancaman di dunia maya dan cara menanggulanginya, sedangkan 20 % yang awalnya tidak tahu menjadi sekedar mengetahui saja. Artinya, materi dapat diterima dan memberikan dampak terhadap

80% peserta seminar. Hal ini ditunjukkan dalam Gambar 4.

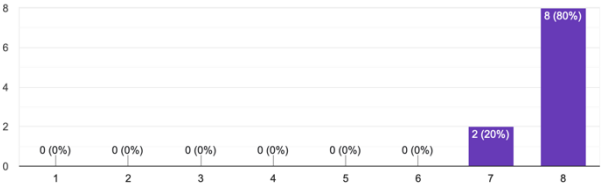


Gambar 3. Peningkatan Pengetahuan Atas Keamanan Digital



Gambar 4. Peningkatan Kesadaran Ancaman dan cara Menanggulangi Kejahatan Digital

Cara sederhana dalam memastikan valid atau tidaknya sebuah informasi adalah dari sumber yang membagikannya. Oleh sebab itu, setelah seminar 80% peserta menyatakan menjadi penting untuk memastikan isi informasi secara keseluruhan dari nomor/sumber yang tidak diketahui. Hasil ini ditunjukkan pada Gambar 5.

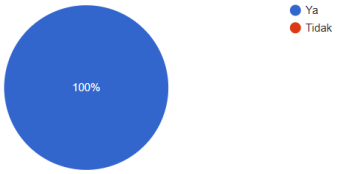


Gambar 5. Kesadaran Memastikan Kebenaran Informasi

Meningkatkan keamanan juga dapat dilakukan dengan penggunaan koneksi internet yang aman. Salah satunya adalah pemanfaatan jaringan wi-fi *public*. Setelah dilaksanakan seminar, peserta menyatakan setuju 100% bahwa mereka tidak akan meng-klik link yang berasal dari sumber yang tidak terpercaya. Hasil ini ditunjukkan pada Gambar 6.

Gambar 6. Tindakan Saat Mendapatkan Link Iming/Iming Hadiah

Keamanan data perlu dijaga dengan menerapkan mengaktifkan *Two Factor Authentication (2fa)* menjadikan sistem akan mengirimkan kode verifikasi melalui metode yang dipilih. Keamanan menjadi hal yang perlu diperhatikan ketika akun dikelola beberapa pengurus yang berbeda. Berdasarkan pernyataan ini, setelah mengikuti seminar, maka 100 % peserta setuju bahwa mereka akan menerapkan pengaman login 2 cara (setelah login, ada SMS/whatsapp nomor aktivasi) atau *Two Factor Authentication (2fa)*. Hasil ini ditunjukkan pada Gambar 7.



Gambar 7. Peserta Menerapkan *Two Factor Authentication (2fa)*

Dalam pelaksanaan seminar juga dilakukan sesi tanya jawab yang ditunjukkan dalam Gambar 9.

Gambar 9. Foto Saat Sesi Diskusi/Tanya Jawab.

D. PENUTUP

Simpulan

Hasil pengabdian kepada masyarakat ini menunjukkan peserta mengalami peningkatan kesadaran terhadap ancaman keamanan digital dengan level pemahaman yang bervariasi. Peserta menjadi lebih sadar akan ancaman kejahatan dan cara menanggulanginya. Ada juga peserta yang mengetahui tentang ancaman kejahatan digital, namun belum dapat menerapkan cara menanggulanginya. Peserta dapat memastikan kebenaran informasi dari nomor atau sumber yang tidak diketahui. Peserta juga menerapkan *Two Factor Authentication (2fa)* untuk perlindungan data dan mereka setuju untuk

tidak meng-klik link yang berasal dari sumber tidak kredibel.

Ucapan Terima Kasih

Terima kasih kepada Lembaga Penelitian dan Pengabdian (LPPM) Universitas Amikom Yogyakarta yang telah mendanai atas keterlaksanaan program ini.

E. DAFTAR PUSTAKA

Darmawan, H. "Kemenkominfo Mencatat Jumlah Pengguna Internet di Indonesia Mencapai 202,35 Juta Orang Artikel ini telah tayang di Tribunnews.com dengan judul Kemenkominfo Mencatat Jumlah Pengguna Internet di Indonesia Mencapai 202,35 Juta Orang,https://tribunnews.c,"2022.https://www.tribunnews.com/techno/2022/01/20/kemenkominfo-mencatat-jumlah-pengguna-internet-di-indonesia-mencapai-20235-juta-orang.

Flatworld Solutions. "10 Tips To Ensure Security of Your Mobile Apps." https://www.flatworldsolutions.com/IT-services/articles/mobile-app-security-tips.php.

Kominfo. (2013). "Kominfo : Beberapa Langkah Pengguna Internet untuk Cegah Penyalahgunaan TIK,".https://www.kominfo.go.id/content/detail/3480/kominfo-beberapa-langkah-pengguna-internet-untuk-cegah-penyalahgunaan-tik/0/berita_satker.

Maulida, L. "Lebih dari 90 Persen Warganet Indonesia Mengakses Internet lewat Ponsel Artikel ini telah tayang di Kompas.com dengan judul 'Lebih dari 90 Persen Warganet Indonesia Mengakses Internet lewat Ponsel',

Social, W. A. (Hootsuite). (2022). "Digital 2022 : Global Overview Report," 2022. https://www.hootsuite.com/resources/digital-trends.